# A Secure Collaborative Spectrum Sensing Mechanism based on User Trust in Cognitive Radio Networks

Sumit Kar
Department of Computer Science Engineering and Application
Indira Gandhi Institute of Technology
Sarang, Odisha, India

Srinivas Sethi
Department of Computer Science Engineering and Application
Indira Gandhi Institute of Technology
Sarang, Odisha, India

## ABSTRACT

The rapid growth of wireless applications has increases the importance for efficient utilization of the scarce spectrum resources. Cognitive Radio Network (CRN) is an emerging technology which leads to solve these problems through dynamic utilization of the unused licensed spectrum. Spectrum sensing is a key function of cognitive radio to find the spectrum holes and Collaborative or cooperative sensing has been proposed to improve the ability. On the other hand, the flexibility in collaborative spectrum sensing opens way to a number of security vulnerabilities. While the set of security challenges in CRN are diverse, this work focus on one of these major threats called Spectrum Sensing Data Falsification (SSDF) attack or Byzantine attack. In SSDF attack, the malicious member of the network sends false sensing reports to the cooperative sensing process and that can break down the normal activities of the whole CRN. This paper presents a novel trust calculation based mechanism that consists of two major steps: Trust value evaluation stage and malicious node detection stage to thwart SSDF attack in the cooperative sensing process of CRN.

## Keywords

Cognitive radio network; Spectrum Sensing Data Falsification (SSDF) attack; Trust; Security threats; Malicious node detection

## 1. INTRODUCTION

Radio spectrum is limited and is a valuable resource for every wireless communication. In the conventional spectrum management (static) policy most of the spectrum is allocated to licensed users for its exclusive use. A survey of spectrum utilization made by Federal Communications Commission (FCC) [1] has found that most of the licensed spectrum is largely under-utilized. To meet the spectrum demands of the increasing wireless applications and for efficient utilization of radio spectrum, FCC has decided to revisit the problem of spectrum management often called Dynamic Spectrum Access (DSA) policy [2]. Where the secondary users operate in the fellow licensed spectrum bands opportunistically called opportunistic spectrum access (OSA).

Over the last decade, Cognitive Radio (CR) has been evolved as an emerging wireless communication paradigm to meet the requirements of the DSA policy. In CRN, users are basically divided in to two categories: (i) Primary Users (SUs) or incumbent users, which holds license to use a particular portion of a spectrum (ii) Secondary Users (SUs) or cognitive users, which are unlicensed users. In CRN, the SUs (unlicensed users) can use the unused PU (licensed user) free spectrum on a non interface basis to it. So when the PU resumes transmission the SU has to vacant the channel immediately.

However, Security is a major concern in CRN, which needs to be addressed thoroughly for getting proper benefit of this novel technology. In this context, this article proposes a trust based model to mitigate SSDF attack in CRN. The organization of the rest of the paper is as follows: In section 2, Preliminaries related on cognitive cycle, Collaborative Spectrum Sensing (CSS) model and security vulnerabilities on CRN are described. Section 3, is contributed to highlight the comprehensive literature review of the related work. The proposed malicious detection technique and algorithm is described in Section 4. Finally the paper concludes including the road map for future work in Section 5.

## 2. PRILIMINARIES

### 2.1 Cognitive Cycle

Cognitive cycle [3] or the operating steps of CRN basically consists of Sense-Analyze-Decide-Adapt functionalities as illustrated in “Fig 1”.

- Spectrum sensing is a key step in CRN, in which the CR users has to reliably sense the spectrum holes. Spectrum sensing techniques include energy detection, cyclostationary feature detection, and Matched filter detection [7]. This article has considered energy detection technique for its simplicity and low computational overhead.
- In second step, based on the available spectrum holes information it analyses various channel and network characteristics like capacity, delay, bit error rate. It then feeds above data to the spectrum decision process.
- Decide is the process of selecting the most appropriate spectrum hole for transmission based on the spectrum characteristics and the Quality of Service requirements (QoS). Spectrum decision can be made by a single CR node or output of a number of CRs cooperatively.
- Adapt stage involves reconfiguration of several characteristics of their physical layer like (i) types of modulation (ii) Transmission power (iii) carrier frequency etc. to adapt to the environment.

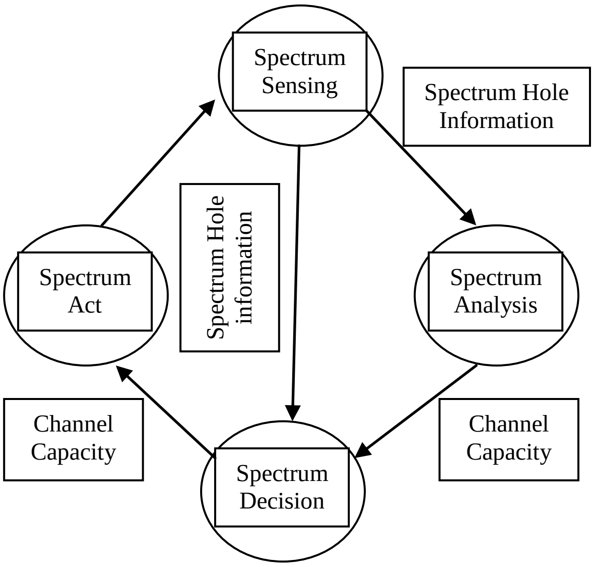

**Fig 1: Cognitive Cycle**

## 2.2 Collaborative Spectrum Sensing

Performing reliable spectrum sensing to detect the spectrum white spaces is a key task in Cognitive radio network. It can be conducted either individually called single user spectrum sensing (local spectrum sensing) or cooperatively. However, due to multipath fading or shadowing effects the single user spectrum sensing is not reliable.

In Collaborative Spectrum Sensing (CSS) [4][5] each user conduct its own local sensing and sends the sensing report to a Fusion Center (FC) as illustrated "Fig 2". The FC combines those local sensing reports to take the final spectrum occupancy decision. The local spectrum sensing has to decide between the hypotheses tests as follows [6].

$$\mathbf{X_i\,(t)} = \begin{cases} \mathbf{n_i\,(t)} & , \ \mathbf{H_0} \\ \mathbf{h_i\,s(t) + n_i\,(t)} & , \ \mathbf{H_1} \end{cases} \quad (1)$$

Where $H_0$ : Primary user is absent
$H_1$ : Primary user is present

$X_i(t)$ is the received signal by the i$^{th}$ cognitive radio at time t, s(t) is the PU signal, $n_i(t)$ is the thermal noise and $h_i$ is the channel gain from PU to i$^{th}$ CR. If the received energy is more than a predefined threshold, it is decided that PU is present otherwise the concerned frequency band is free. Thus, the local sensing report $u_i$ of i$^{th}$ CR at t$^{th}$ sensing period is expressed as a binary variable as follows:

$$\mathbf{u_i^t} = \begin{cases} \mathbf{0} & , \ \mathbf{H_0} \\ \mathbf{1} & , \ \mathbf{H_1} \end{cases} \quad (2)$$

## 2.3 Security Threats in Cognitive Radio Network

As the CRN technology evolved day by day, providing proper security to this novel technology has becomes a major concern. Like conventional wireless networks, cognitive radio networks are also vulnerable to the traditional security threats such as Denial of Service (DoS), selfish misbehaviours, jamming attack, sinkhole attack etc [16]. In addition, CRN introduces significant new classes of security threats and vulnerabilities due to its unique characteristics and functioning techniques [7] [8] [17]. The CRN specific attack includes Spectrum Sensing Data Falsification (SSDF) or Byzantine attack, Primary User Emulation (PUE) attack, Common Control Channel (CCC) attack, Objective Function Attack (OFA) etc.

This work focus on one of the major CRN specific security called spectrum sensing data falsification (SSDF) or Byzantine attack [4][5][9]. In SSDF attack, the malicious node of the network forwards false sensing report to the cooperative sensing process as illustrated in "Fig 2". This can severely affect the performance of the CSS system by taking a wrong status decision about the spectrum band. This may cause either interference with the PU or results under utilization of the spectrum usage. Therefore, it is a challenging issue to design an efficient secure CSS system in CRN to detect such malicious users and isolate their sensing reports before the fusion.

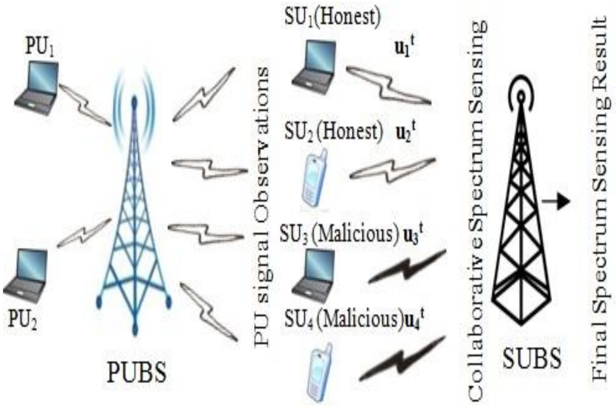
PU$_1$
PU$_2$
PUBS
PU signal Observations
SU$_1$(Honest) $u_1^t$
SU$_2$(Honest) $u_2^t$
SU$_3$(Malicious) $u_3^t$
SU$_4$(Malicious) $u_4^t$
Collaborative Spectrum Sensing
SUBS
Final Spectrum Sensing Result

**Fig 2 : Collaborative Sensing and SSDF Attack**

## 3. RELATED WORK

Security is one of major concern in CRN because of the importance of CR network reliability. In addition to all the advantages of CSS process, it introduces security vulnerability like SSDF attack. In SSDF attack, some malicious nodes send false sensing data to the FC in an intention to use the idle spectrum selfishly or to cause interference with the PU. There are several countermeasures have been proposed to detect and mitigate SSDF attack or byzantine attack in CRN.

Studies in [7] [8][17], shown the details analysis of the major possible attacks in CRN paradigm. The authors in [4], apply an average combination scheme to combine the local sensing data of users. To detect malicious users, it first uses a pre-filtering step to identify and remove the permanent malicious nodes like the 'Always Yes' and the 'Always No' type. Next, by calculating the trust factor of users based on their past and present sensing reports it identifies the rest outliers.

In [10], the authors analyze two different types of collusive or cooperative SSDF attack models known as Vicious Collusive SSDF (VC-SSDF) attack and Rational Collusive SSDF (RC-SSDF) attack. Considering both the above attack models, proposed a trust-based defence scheme called Sensing guard. Basically sensing guard consists of three operating stages like data management stage, trustworthiness evaluation stage and lastly the attacker detection stage. The main outcome of the presented work is the evaluation of user's trustworthiness by considering multiple PU.

In [11], discuses both the independent and cooperative SSDF attack scenario in CRN. To detect SSDF attack, they proposed a reputation-based clustering algorithm. The simulations results shows that the proposed approach can efficiently detect both the independent and cooperative SSDF attacks. However, when the number of independent attackers increases significantly it may not provide the better result.

In the paper [12], the authors proposed a malicious user detection technique using conditional frequency check (CFC) statistics and an auxiliary hamming distance check (HDC). Attacker detection as well as imposing punishment called Security Management based on Trust Determination (SMTD) mechanism is presented by [13]. The proposed mechanism consists of six functions: authentication, interactive, configuration, trust value collection, storage and update, and punishment.

Fast Probe, an active transmission based algorithm for detecting SSDF attack by using PUE signals has been introduced in [14]. In addition with detecting those malicious SUs sending false sensing reports it can also detect those SUs that do not perform in-band sensing.

The work in [15] determines the trustworthiness of each SU participating in the CSS approach for a centralised CRN. The calculation is based on by considering both the sensing reputation and etiquette reputation of a particular participant. Finally, both the reputation values are considered in the data fusion process and channel allocation among the SUs.

## 4. THE PROPOSED APPROACH

This section makes a detailed analysis of the proposed trust based technique to detect and mitigate SSDF attack in CRNs.

Since, the future behaviour prediction of a user is based on its past activities; in this work the past and present sensing reports are used as a measure to differentiate the normal, honest and malicious users. Accordingly referring to the “Fig 3” the sensing reporting history during the past sensing period T of a SU is used to predict its future behavior in the coming time interval $(t_{n+1}, t_{n+2})$. The proposed model consists of two major steps: Trust value evaluation stage and to malicious node detection stage.

### 4.1 Trust Value Evaluation

In this paper, the past history of sensing data provided by each SU, for a particular PU are recorded separately by the FC called sensing history record as shown in Table 1.

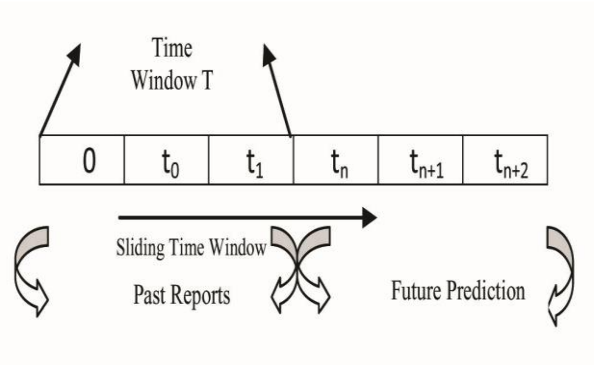

**Fig 3: Sensing Time Window**

**Table 1. Sensing History Record**

| Sensing Period | $SU_1$ | $SU_2$ | … | $SU_n$ | $PU_i$ |
|---|---|---|---|---|---|
| 1 | $u_1^1$ | $u_2^1$ | … | $u_n^1$ | D(1) |
| 2 | $u_1^2$ | $u_2^2$ | … | $u_n^2$ | D(2) |
| … | … | … | … | … | … |
| t | $u_1^t$ | $u_2^t$ | … | $u_n^t$ | D(t) |

The sensing history record table is based on the concept of sliding timing window as illustrated in “Fig 3”. Thus, after completion of a sensing period, the sliding time window slides one unit to the right and thus, removes the history T times ago. Hence, the sliding time window always contains the sensing report history of last T sensing periods.

Let the set of correct spectrum reports from sensing periods 1 to t by SU $u_n$ for the $PU_i$ i.e. the number of times the final sensing decision D(i) was similar to the local decision by $u_n$ is denoted as $u_n+ = \{u_n^R \mid u_n^R Є u_n\}$. Similarly the set of incorrect spectrum reports from sensing periods 1 to t by SU $u_n$ for the $PU_i$ i.e. the number of times the final sensing decision D(i) was different to the local decision by $u_n$ is denoted as $u_n^- = \{u_n^W \mid u_n^W Є u_n\}$.

Next based on the sensing history stored in Table 1, the trustworthiness of each SU is calculated using (3). The range of trust value T is represented by 0 ≤ T ≤ 1, where 0 denotes complete distrust and 1 denotes complete trust. In the current sensing period t, the trust value of SU $u_n$ on $PU_i$ is calculated as follows:

$$T'[u_n{}^t] = \frac{\left|u_n{}^+\right|}{\left|u_n{}^+ + u_n{}^-\right|} \tag{3}$$

Further, the average trust value of $u_n$ by considering the sensing history on all the PUs in the network can be calculated as follows:

$$T\left[u_n{}^t\right] = \frac{1}{k}\sum_{0}^{k} T'[u_n{}^t] \tag{4}$$

Where K= Number of PUs present in the network.

### 4.2 Malicious Node Detection

In a networking system it is difficult to predict the normal and the abnormal behaviors, as the boundaries cannot be well defined. In this proposed model, based on the calculated average trust value $T[u_n^t]$ of CR users, five trust levels are defined, where each trust level represents the degree of reliability of a node i.e. honest, malicious or suspicious as shown in Table 2.

**Table 2. Trust Level of Cognitive Radio**

| Trust Level | Trust Values | Meaning |
|---|---|---|
| Highest | 0.9 - 1 | Honest |
| High | 0.8 – 0.89 | Honest |
| Medium | 0.6 - 0.79 | Suspicious |
| Low | 0.4 - 0.59 | Malicious |
| Lowest | 0 – 0.39 | Malicious |

Further, the proposed malicious node detection technique involves two major steps as discussed below. The details proposed malicious node detection approach is summarized in algorithm 1.

***Algorithm 1: Malicious user detection algorithm***

```
For each SU from 1 to n do
    For on each PU from 1 to K do
        Calculate the trust values $T'[u_n^t]$;
        Calculate the average trust value $T[u_n^t]$;
    If $T[u_n^t] \geq 0.8$;
    Then
        Honest user; break;
    End
    Else if $T[u_n^t] < 0.6$;
    Then
        Malicious user; break;
    End
    Else
        Suspicious user;
        If each $T'[u_n^t] \geq \mu$;
        Then
            Honest user; break;
        End

        Else
            Malicious user; break;
        End
     End
     End
End
```

***Step I:***

If the calculated trust level is highest or high i.e. $T[u_n^t] \geq 0.8$, then the CR user is declared as honest. Thus, its current sensing report is being accepted and sent to the FC for fusion. Secondly, if the trust level is low or lowest i.e. $T[u_n^t] < 0.6$, then the CR user is declared as malicious and its current sensing report is being discarded. The intention of Step-I is to separate the complete honest users and filtered out the extreme malicious users. The remaining user comes under suspicious category and needs further verification in Step-II. The whole concept of Step-I can written as

$$u_n = \begin{cases} \textit{Honest} \text{ if } T[u_n^t] \geq 0.8 \\ \textit{Suspicious} \text{ if } 0.6 \leq T[u_n^t] < 0.8 \\ \textit{Malicious} \text{ if } T[u_n^t] < 0.6 \end{cases} \qquad (5)$$

***Step II:***

If the trust level is medium, then the CR user is declared as suspicious and needs further verification. These kinds of users are may belongs to the intelligent malicious type; which give correct sensing reports for all the PU, except the PU which it wants to use exclusively. To detect such intelligent malicious users, define a threshold μ and compare it with the calculated individual trust value $T'[u_n^t]$ of the concerned SU. If the suspicious user's trust value on any PU is less than μ, it is declared as malicious otherwise declared as honest. Thus, if a malicious user is reporting wrongly only for some specific PU, will detect as follows:

$$u_n = \begin{cases} \textit{Honest} \text{ if each } T'[u_n^t] \geq \mu \\ \textit{Malicious} \text{ if any } T'[u_n^t] < \mu \end{cases} \qquad (6)$$

The suspicious users which are finally declared as honest users after (6), their current spectrum sensing reports are accepted by the FC for fusion. Otherwise declared as malicious user and their sensing results are discarded.

## 4.3 Case Study

To further discuss the feasibility of the above proposed malicious node detection technique, a case study is designed as [10].

Let the CRN has 5 cooperative SUs namely $SU_1$, $SU_2$, $SU_3$, $SU_4$ and $SU_5$ and 3 PUs namely $PU_1$, $PU_2$ and $PU_3$. Next the sensing report history of each SU with respect to 3 PUs is assumed to as follows:

**Table 3. $PU_1$ Table**

| Sensing Period | $SU_1$ | $SU_2$ | $SU_3$ | $SU_4$ | $SU_5$ | $PU_1$ |
|---|---|---|---|---|---|---|
| 1 | 1 | 0 | 0 | 1 | 1 | 1 |
| 2 | 1 | 0 | 1 | 1 | 1 | 1 |
| 3 | - | 0 | 0 | 0 | 0 | 0 |
| 4 | 1 | 0 | 0 | 1 | 0 | 0 |
| 5 | 1 | 0 | 1 | 1 | 1 | 1 |

**Table 4. $PU_2$ Table**

| Sensing Period | $SU_1$ | $SU_2$ | $SU_3$ | $SU_4$ | $SU_5$ | $PU_2$ |
|---|---|---|---|---|---|---|
| 1 | 1 | 0 | 1 | 0 | 0 | 0 |
| 2 | 1 | 0 | 0 | 1 | 1 | 1 |
| 3 | 1 | 0 | 1 | 0 | 1 | 1 |
| 4 | 1 | 0 | 0 | 1 | 0 | 0 |
| 5 | 1 | 0 | 0 | 1 | 0 | 0 |

**Table 5. $PU_3$ Table**

| Sensing Period | $SU_1$ | $SU_2$ | $SU_3$ | $SU_4$ | $SU_5$ | $PU_3$ |
|---|---|---|---|---|---|---|
| 1 | 1 | 0 | 0 | 1 | 1 | 1 |
| 2 | 1 | 0 | 1 | 0 | 1 | 1 |
| 3 | 1 | 0 | 0 | - | 0 | 0 |
| 4 | - | 0 | 0 | 1 | 1 | 1 |
| 5 | 1 | 0 | 0 | 0 | 0 | 0 |

Where "0" denotes the concerned PU is absent and "1" denotes the concerned PU is present. Based on the sensing history report stored in Table 3, Table 4 and Table 5, the trust values of $SU_i$ on each $PU_i$ is calculated using "(3)". Further, the average trust value of each $SU_i$ is obtained by taking the average of the above calculated trust values referring "(4) "as follows:

$T[su_1]= 0.55$, $T[su_2]= 0.46$, $T[su_3]= 0.66$, $T[su_4]= 0.65$, $T[su_5]= 1$.

Next, after verifying the above calculated average trust value of SUs, map it to a particular trust level referring to the Table 2 and differentiate the normal, malicious and suspicious nodes. Accordingly it can find that $SU_1$, $SU_2$ are malicious and $SU_3$, $SU_4$ are suspicious and $SU_5$ is found to be normal. To further verify the suspicious users $SU_3$, $SU_4$, the threshold μ is taken as 0.6. It is found for $SU_3$, $T^1[su_3]=0.8$, $T^2[su_3]=0.6$ and $T^3[su_3] =0.6$ and for $SU_4$, $T^1[su_4]=0.8$, $T^2[su_4]=0.4$ and $T^3[su_4] =0.75$. Referring to (5), $SU_3$ is declared as honest and $SU_4$ is declared malicious as $T^2[su_4] < 0.6$.

Thus, finally the current sensing reports of $SU_1$, $SU_2$ and $SU_4$ are discarded and sensing reports of $SU_3$ and $SU_5$ are taken up for fusion by the FC.

## 5. CONCLUSION

This paper, proposed a secure collaborative sensing framework in cognitive radio network using user trust calculation. Unlike the existing mechanisms, the proposed scheme evaluates the trustworthiness of each SU by considering different PUs. The future researches are to simulate the suggested model and intend to measure the stability of the approach with variation in number of malicious user in the network. Further research could focus on to study the effect of cooperation among malicious users in CRN. In addition, extending the trust based system to other steps of cognitive cycle is another direction for further research.

## 6. REFERENCES

[1] "Spectrum policy task force report". Technical Report, FCC ET Docket 02-135, Federal CommunicationsCommission, Nov 2002.

[2] R. Chen, J. Park, and K. Bian. "Robust distributed spectrum sensing in cognitive radio networks," In proc. of IEEE Conference on Computer Communications (INFOCOM), pp. 1876-1884, 2008.

[3] I.F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty. "Next gener-ation/ Dynamic spectrum access/ Cognitive radio wireless networks: A survey," Computer Networks, 50(13), pp.2127-2159, May 2006.

[4] P. Kaligineedi, M. Khabbazian, and V. K.. Bhargava, "Secure cooperative sensing techniques for cognitive radio systems,". In Proceedings of IEEE International Conference on Communication, pp. 3406-3410, IEEE, May 2008.

[5] W. Wang, H. Li, Y. Sun, and Z. Han, "Attack-proof collaborative spectrum sensing in cognitive radio networks," In CISS, pp. 130-134. IEEE, March 2009.

[6] W. Wang, H. Li, Y. Sun, and Z. Han, "Catchit: Detect malicious nodes in collaborative spectrum sensing," In GLOBECOM, pp. 1-6. IEEE, 2009.

[7] A. Attar, H. Tang, A. V. Vasilakos, F. R. Yu, and V. C. M. Leung. "A survey of security challenges in cognitive radio networks: Solutions and future research directions," Proceedings of the IEEE, 100(12), pp. 3172-3186, December 2012.

[8] A. G. Fragkiadakis, E. Z. Tragos, and I.. G. Askoxylakis. "A survey on security threats and detection techniques in cognitive radio networks". IEEE Communications Surveys and Tutorials, 15(1), pp. 428-445, 2013.

[9] A. S. Rawat, P. Anand, H. Chen, and P. K. Varshney, "Countering byzantine attacks in cognitive radio networks," In ICASSP, pp. 3098-3101, IEEE, 2010.

[10] J. Feng, Y. Zhang, G. Lu and L. Zhang, "Defend against Collusive SSDF Attack Using Trust in Cooperative Spectrum Sensing Environment," 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, pp.1656-1661, 2013.

[11] L. Li, F. Li and J. Zhu, "A method to defense against cooperative SSDF attacks in Cognitive Radio Networks," In Signal Processing, Communication and Computing (ICSPCC), 2013 IEEE International Conference on, pp.1-6, 2013.

[12] X. He, H. Dai and P. Ning, "A byzantine attack defender in cognitive radio networks: the conditional frequency check," IEEE Transactions on Wireless Communications, Vol. 12,No. 5, pp.2512–2523, 2013.

[13] J. Li, Z. Feng and Z. Wei, Z. Feng and P. Zhang, "Security management based on trust determination in cognitive radio networks," EURASIP J. Adv.Sig. Proc.,48 ,pp. 1-16, 2014.

[14] T. Bansal and B. Chen and P. Sinha, "FastProbe: Malicious user detection in Cognitive Radio Networks through active transmissions," IEEE Conference on Computer Communications, INFOCOM 2014, pp. 2517-2525, 2014.

[15] Q. Pei, B. Yuan, L. Li and H. Li, "A sensing and etiquette reputation-based trust management for centralized cognitive radio networks," Neurocomputing, 101, pp.129-138 ,2013.

[16] D. Martins and H. Guyennet (2011). "Security in wireless sensor networks: a survey of attacks and countermeasures", International Journal of Space-Based and Situated Computing, 1(2-3), pp.151-162, 2011.

[17] S.Kar, S. Sethi and M.K. Bhuyan, "Security challenges in cognitive radio network and defending against Byzantine attack: a survey", Int. J. Communication Networks and Distributed Systems, Vol. 17, No. 2, Inderscience, pp.120–146, 2016.